

UNIVERSITAS BINA NUSANTARA

Program Ganda
Teknik Informatika – Matematika
Skripsi Sarjana Program Ganda
Semester Ganjil 2010/2011

PERANCANGAN PROGRAM SIMULASI PENGAMANAN DATA TRANSMISI PADA *CONTACTLESS SMART CARD* DENGAN METODE *SERPENT AES*

Santi Gowani
1000870432

ABSTRAK

Perkembangan ilmu pengetahuan dan teknologi informasi sangat membantu dalam kemudahan hidup manusia. Salah satunya adalah *Contactless Smart Card* yang banyak digunakan untuk menyimpan data-data berupa informasi penting dan bersifat rahasia seperti identitas seseorang dan data perbankan. Pertukaran informasi pada *Contactless Smart Card* dianggap rentan karena ditransmisikan melalui gelombang radio sehingga harus diamankan terlebih dahulu sebelum dikirimkan. Cara pengamanan data transmisi melalui gelombang radio pada *Contactless Smart Card* adalah dengan kriptografi menggunakan metode *Serpent AES*.

Tujuan perancangan ini adalah membuat sebuah program simulasi yang akan digunakan untuk mengamankan data transmisi pada *Contactless Smart Card* dengan metode *Serpent AES*. *Serpent AES* ini melakukan 32 tahap *SP-Network* yang dioperasikan dengan 8 *S-Box* untuk mendapatkan data yang aman sehingga siap untuk ditransmisikan pada *Contactless Smart Card*. Program simulasi ini melakukan pengamanan terhadap data yang akan ditransmisikan ke dalam *Contactless Smart Card*. Sedangkan untuk proses konversi digital ke analog dan transmisinya sendiri tidak dilakukan oleh program simulasi ini, karena merupakan bagian kinerja *hardwere*. Pada program simulasi ini, ditunjukkan juga bahwa yang dikriptografi bukan hanya *plain text* melainkan juga berbentuk *file*.

Kata Kunci : *Smart Card*, *Contactless Smart Card*, RFID, *Serpent AES*, Pengamanan Data Transmisi, Kriptografi.